

**REMARKS**

Claims 1-32 are pending in the present application.

This Amendment is in response to the Office Action mailed January 17, 2007. In the Office Action, the Examiner rejected claims 1-8, 17-32 under 35 U.S.C. § 101, and claims 1-32 under 35 U.S.C. § 103(a).

Applicant has amended claims 1, 9, 17 and 25, added claims 33-35. Applicant submits that the newly added claims introduce no new matter. Reconsideration in light of the amendments and remarks made herein is respectfully requested.

**I. REJECTIONS UNDER 35 U.S.C. § 101**

In the Office Action, the Examiner rejected claims 1-8, 17-32 under 35 U.S.C. § 101 because the claimed invention is directed to non-statutory subject matter. Specifically, the Examiner stated, “[C]laim 1 discloses a method for generating a shared key that includes performing a first and second exponentiation operation to generate a key. The claimed method is directed to an abstract idea because the claim does not require any physical transformation and the invention do not produce a useful, concrete, and tangible result.” Applicant respectfully traverses the rejection for the following reasons.

A claimed process is statutory if it is limited to a practical application of the abstract idea or mathematical algorithm in the technological arts. See Alappat, 33 F.3d at 1543, 31 USPQ2d at 1556-57 (quoting Diamond v. Diehr, 450 U.S. at 192, 209 USPQ at 10). See also Alappat 33 F.3d at 1569, 31 USPQ2d at 1578-79 (Newman, J., concurring) (“unpatentability of the principle does not defeat patentability of its practical applications”) (citing O'Reilly v. Morse, 56 U.S. (15

How.) at 114-19). A claim is limited to a practical application when the method, as claimed, produces a concrete, tangible and useful result; i.e., the method recites a step or act of producing something that is concrete, tangible and useful. See AT&T, 172 F.3d at 1358, 50 USPQ2d at 1452. MPEP 2106 IV.B.2.

Claims 1, 17, and 25 recite, inter alia, performing the first exponential operation to generate a first public key..., performing a second exponential operation to generate a shared secret key..., performing a third exponential operation to generate the shared secret key, providing a first certificate..., providing a second certificate..., etc., The “shared key”, “parameters”, “certificates”, etc. represent concrete and tangible entities. The operation “performing exponential operations”, “providing”, etc. perform transformations to produce concrete, tangible, and useful results. This claimed process is statutory since it is limited to a practical application and the process produces concrete, tangible and useful results.

Claims should be interpreted consistently with the specification, which provides content for the proper construction of the claims because it explains the nature of the patentee’s invention. See Renishaw P.L.C. v. Marposs Societa Per Azioni, 158 F.3d 1243 (Fed. Cir. 1998).

The claimed invention is directed to generating a shared secret key for a first peer (i.e., client) using a public key (i.e., generates from parameter of a first certificate...) from a second peer (i.e., server) and a private key from the first peer. The “certificate” is an electronic document (page 11, line 7), “private key” stored in a flash memory (page 13, lines 6-7), “public key” is kept in file (page 9, line 21-22) show “tangible and concrete” (Figure1). All elements of the claims are concrete, tangible, and useful. The operations of generating first, second, and third

exponential operations that generate a shared key for the client using the public key from the server and the private key from the client produce concrete, tangible, and useful results. Moreover, the first and second peers are communicated via a network. This, alone, produces concrete, tangible, and useful results.

Accordingly, Applicant submits that claims 1-8 and 17-32 are statutory under 35 U.S.C. § 101 and respectfully requests the rejection be withdrawn.

## **II. REJECTIONS UNDER 35 U.S.C. § 103**

The Examiner rejected claims 1-32 under 35 U.S.C. § 103(a) as being unpatentable over U. S. Patent No. 6,931,528 issued to Immonem ("Immonen"). Applicant respectfully traverses the rejection for the following reasons.

Immonen discloses certificate  $C_A$  and certificate  $C_B$  (Figs. 1 & 2 and Col. 3, lines 11 & 20). Instead of requesting A's certificate from A itself, the server B uses the  $ID_A$  sent by A to retrieve A's certificate from a certificate store CS (Col. 3, lines 9-16). B verifies  $C_A$ , obtains A's public key  $E_A$  and calculates the shared secret key. B sends to A a second inter-party message which comprises  $C_B$ . A then verifies B's certificate  $C_B$ , obtains B's public key  $E_B$  and calculates the shared secret key. A sends B a third inter-party message comprising a finished message which indicates that it has been able to verify B's certificate (Col. 3. lines 17-27). Moreover, Immonen discloses that with the RSA and ECES algorithms, a server key exchange takes place by B generating a random number, which is a pre-master secret (Col. 3, lines 58-60). Immonen further discloses one-way functions and examples of these functions are multiplying large prime numbers, discrete exponentiation, elliptical functions and hash functions.... (Col. 4, lines 31-41). Immonen may have disclosed a first certificate (i.e.,  $C_A$ ) and a second certificate

(i.e., C<sub>B</sub>). No where in Immonen that discloses a public key is generated using at least one parameter of the first certificate and a private key of the second peer (i.e., B). Applicant is well aware that there are parameters in a certificate as also disclosed in Immonen. Immonen, however, does not use at least one of the parameters in first peer's certificate (i.e., C<sub>A</sub>) to generate a public key. Further, these parameters in the present invention are the digital signature standard (DSS) parameters where Immonen does not disclose that the parameters in the first certificate are DSS parameters.

Immonen, taken alone or in any combination, does not disclose, suggest, or render obvious the use of the at least one parameter of the first peer's parameters together with a private key from the second peer to generate a public key. This aspect of the invention is supported in the specification on paragraphs 0033 and 0040 and is recited in amended claims 1, 9, 17, and 25.

Therefore, Applicant believes that independent claims 1, 9, 17, 25 and their respective dependent claims are distinguishable over the cited prior art references. Accordingly, Applicant respectfully requests the rejections under 35 U.S.C. § 103(a) be withdrawn.

**CONCLUSION**


In view of the amendments and remarks made above, it is respectfully submitted that the pending claims are in condition for allowance, and such action is respectfully solicited. If it is believed that a telephone conversation would expedite the prosecution of the present application, or clarify matters with regard to its allowance, the Examiner is invited to contact the undersigned attorney at the number listed below.

The Commissioner is hereby authorized to charge payment of any required fees associated with this Communication or credit any overpayment to Deposit Account No. 04-1175.

Respectfully submitted,

DISCOVISION ASSOCIATES

Dated: 4/16/07

  
\_\_\_\_\_  
Caroline T. Do, Esq.  
Reg. No. 47,529

DISCOVISION ASSOCIATES  
INTELLECTUAL PROPERTY DEVELOPMENT  
2265 E. 220<sup>th</sup> Street  
Long Beach, CA 90810  
(310) 952-3300